Delta University Scientific Journal
Journal home page: https://dusj.journals.ekb.eg

IoT Based Intrusion Detection Systems from The Perspective of Machine and Deep Learning: A Survey and Comparative Study

Eman Ashraf 1,2, *, Nihal F. F. Areed 2,3, Hanaa Salem 1, Ehab H. Abdelhay 2 and Ahmed Farouk 4

[1] *Department of Electronics and Communications Engineering, Faculty of Engineering, Delta University for Science and Technology, Gamasa 35712, Egypt; eman.ashraf@deltauniv.edu.eg (E.A) hana.salem@deltauniv.edu.eg (H.S)*

[2] *Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt; nahoolaf@mans.edu.eg (N.F.F.A.); ehababdelhay@mans.edu.eg (E.H.A.)*

[3] *Centre for Photonics and Smart Materials, Zewail City of Science and Technology, Giza 12578, Egypt*

[4] *Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University, Hurghada 84511, Egypt; ahmed.farouk@sci.svu.edu.eg*

* Correspondence: Eman Ashraf rashad; Tel.: +20-01003013758; Email: eman.ashraf@deltauniv.edu.eg or engemanashraf23@gmail.com ;

ABSTRACT

The term "Internet of Things" (IoT) refers to a group of gadgets that are capable of connecting to the Internet in order to gather and share data. The growth of Internet connections and the arrival of new technologies like the Internet of Things (IoT) have increased the privacy and security threats associated with the introduction of various gadgets. In order to increase the detection of cyber-attacks, industries are increasing their research spending. Institutions choose wise testing and verification techniques by comparing the highest rates of accuracy. IoT use has been accelerating recently across a variety of industries, including health care, smart homes, intelligent transportation, smart cities, and smart grids. where technology researchers and developers started to take notice of the IoT possibilities. Unfortunately, the privacy and security concerns imposed on by energy restrictions and the scalability of IoT devices present the most significant challenge to IoT. Therefore, how to address the IoT's security and privacy challenges remains an essential issue in the field of information security. With a decentralized design, edge computing plays a vital role in enabling IoT devices to compute, make decisions, take actions, and push only pertinent information to the cloud. Since sensitive data is more readily available and can be used right away, the IDS performs better when employing machine learning (ML) and deep learning (DL) algorithms to identify and prevent various threats. In terms of technical limitations, this study classifies the current, recent research in IoT intrusion detection systems employing machine learning, deep learning, and edge computing architecture.

Keywords: *(Intrusion detection system (IDS), Internet of things (IoT), Machine learning, Deep learning, Anomaly detection)*

1. Introduction

In recent years, the Internet of Things has seen explosive expansion in industry-specific applications like healthcare, transportation infrastructure, smart agriculture, and industries to enhance economic growth [1]. These Internet of Things (IoT) systems consist of a large number of networked sensors, actuators, and various network-enabled devices [2] that exchange various types of data across both the public Internet and private networks. By 2025, the IoT is expected to have an average of 75.3 billion actively connected devices, according to Cisco research [3,4]. IoT technology differs from conventional Internet technology in that human intervention is not required during data sharing between systems. The need for data network bandwidth has expanded along with the growth of IoT devices. However, the majority of IoT devices have resource limitations, making it difficult to implement the conventional system security approaches. The majority of IoT devices, however, have resource limitations, making it difficult to implement traditional security techniques for system protection against cyberattacks. In order to overcome the resource-constraint issues in IoT systems, edge computing—which enables computation to be conducted at the network end—must be introduced [5,6]. IoTs can transfer very computationally heavy operations to the local edge server thanks to edge computing [7]. It is important to consider cyber-security seriously since the IoT has evolved into the engine of the present industrial revolution and the system for gathering live sensitive data

[8,9]. To secure the IoT network and the systems built on it, an Intrusion Detection System (IDS) that can detect existing and upcoming cyberattacks is required.

A number of surveys on various IoT security-related research areas, such as security frameworks [10], healthcare security [10], privacy concerns [11], state of the art and security issues [12], models, methods, and tools [13], and attacks [14], have been published. Some of these articles were released when IoT systems were still in their beginnings. The application of ML approaches to improve IoT security is the main topic of this study.

We also look into how the development of edge computing can help with the creation of an efficient security system (IDS) for IoT systems. This work also contributes to our understanding of the implementation approaches, the IoT dataset used, and the state-of-the-art IDS design for resource-constrained IoT employing the edge and cloud computing.

The research expands on the design strategies employed by researchers and shows how the suggested methods work with IDS design for IoT systems with edge and cloud advances. We also illustrated various options for selecting IDS for IoT devices depending on a few factors. Results from a study of the relevant research articles in this area, the following views are used to serve the researchers:

• presenting and discussing the main significant IoT issues that have arisen in current research trends.
• discussing the ML-based IDS developed for the Internet of Things and their implementation methods.
• In this survey, we discuss the placement strategies utilized to create IDS for IoT systems and evaluating the feasibility of developing security mechanisms for the IoT using edge technology.
• presenting several metrics and datasets that were utilized to produce IDS for IoT systems.

2. IoT Architecture and Security Threats

More progress in IoT systems and applications are expected than anyone could probably predict [15]. However, IoT technology development is still growing and has not reached its full security protection capability. Multiple security issues with IoT systems exist [14], as shown in Figure 1.

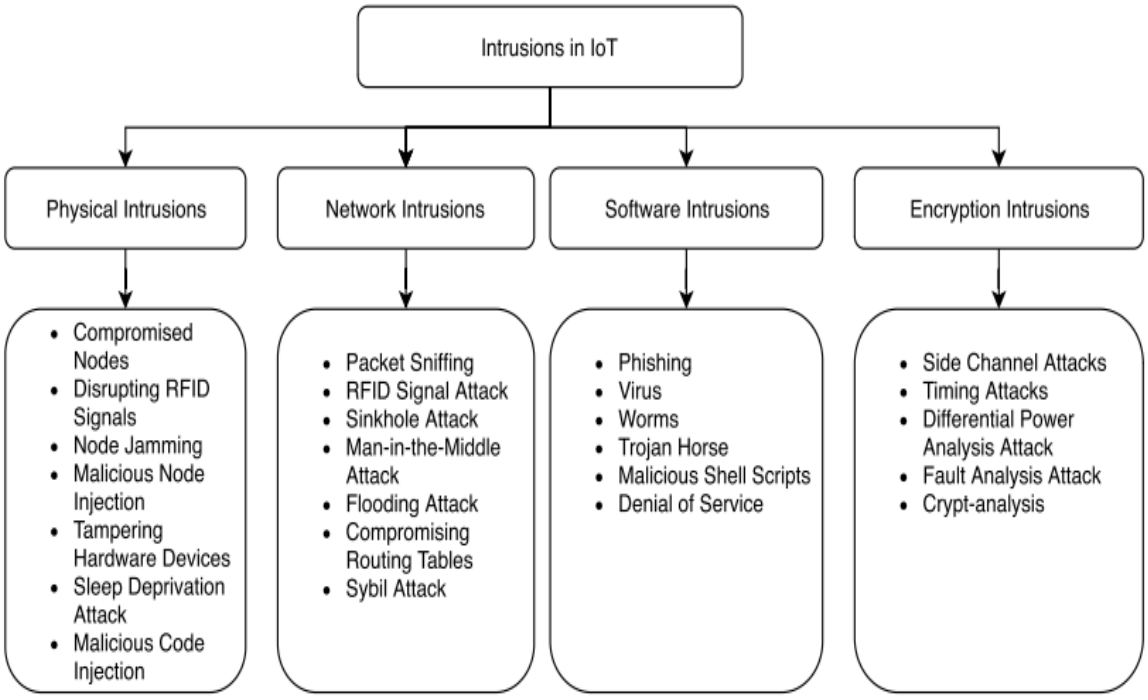

Figure 1: Intrusions in IoT networks

Due to the IoT system applications' rapid spread of technology usage, several network attacks have also arisen [16]. Additionally, the IoT community does not adopt a standard specified security architecture. Depending on the use case, system requirements, available technology, and IoT network scale, various security designs are implemented. For instance, the authors suggested various intelligent security architectures to monitor and track patients' medical information in the intelligent health use cases covered in the research papers in [17]. Data sensitivity varies among IoT use cases.

As a result, creating security for each circumstance needs particular application knowledge. Thus, it is clear that NIDS built to address the varied IoT architectures and use cases need adaptation [18]. The network and infrastructure of IoT systems must also be protected, in addition to using encryption techniques to secure data transmission. Unfortunately, the nature of the resource limitations prevents the use of traditional network security mechanisms in IoT systems. Table 1 shows the attacks have been performed against IoT systems in the recent years.

Table 1: Recent attacks against IoT systems

Type	Description	Attack mode
Spoofing attack	To take over or gain unauthorized access to a network, attackers pretend to be a legitimate Internet of Things system. Attackers launch DoS and Man-in-the-Middle cyberattacks against targeted devices once they have access [19].	Impersonation
Denial of Service (DoS)	A cyberattack renders IoT resources or systems unreachable to the intended authorised users of the network. The purpose of these attacks is to temporarily or permanently interrupt the functions of a host IoT system [20-21].	Network Flooding
Distributed denial-of-service (DDoS)	This attack has the potential to interfere with both normal traffic and the services provided by the network. It saturates a target's or the neighborhood's infrastructure with extremely heavy network traffic [22]. When attackers use several compromised computing systems as the sources to produce a lot of network traffic, DDoS attacks are successful. [23, 24].	Network Flooding
Jamming attack	The majority of IoT devices use wireless networks to connect to other devices. Attacking the targeted IoT system, the culprits deplete its memory, processing power, and bandwidth by sending a phone signal to break up radio communication [25, 26].	False signals
Man-in-the-middle attacks	attackers eavesdrop on the participants' private conversations while covertly relaying and manipulating the communication between two IoT systems and remote devices [27, 28].	Message Eavesdropping
Mirai attack	Using malware called Mirai, cybercriminals can use networked devices as part of a botnet in a wide network that can be remotely controlled. It primarily targets online consumer electronics, including	Injecting malware on devices

	routers and IP cameras. Mirai was frequently used as an initiator in attacks like DoS/DDoS [29, 30].	
Sybil Attack	alters the identity of the IoT device to generate numerous anonymous identities and use an excessive amount of power. It was given that name in honour of Sybil, who wrote the book Sybil, a case study of a lady coping with dissociative identity disorder. [31, 32].	creation of anonymous identities

3. ML Based Intrusion Detection Systems for IoT networks

An IoT network's device-to-device traffic packets is monitored by IDS. It serves as a line defense that can detect dangers and prevent the network from unauthorized access and malicious attacks. The main defense against network intrusion and other threats in modern computer networks is IDS.NIDS analyses and examines the network and logins on the hosted device and finds signatures of known threats and unknown dangerous malware attacks on a network itself. Monitoring the IoT network, identifying illegal intrusions, and enabling context-awareness to other systems devices linked to the network and taking the required defensive measures, are other objectives of the IDS. When IDS detects both internal and external threats, it will also generate an alert or set up attack flags, Figure 2 shows the components of IDS.

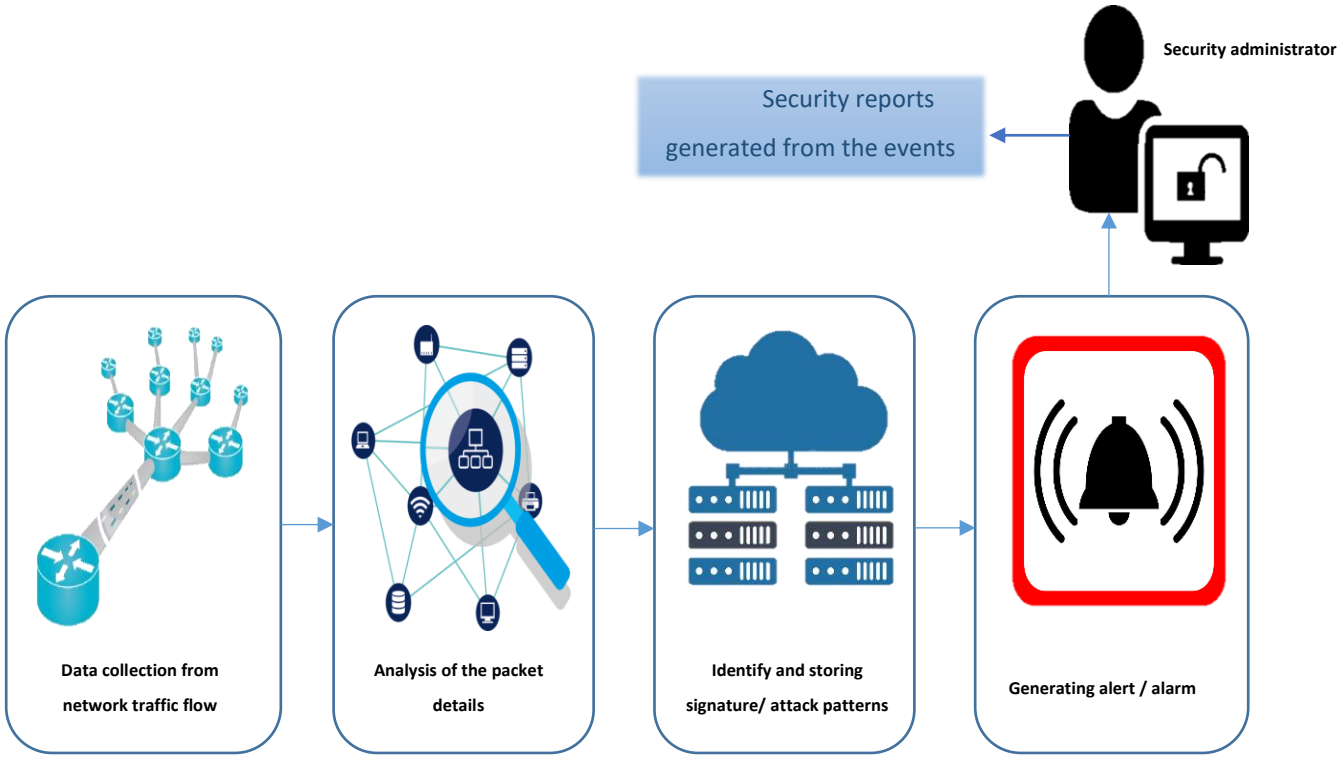

Figure 2: Components of intrusion detection systems

Through the network-connected IoT devices that have been compromised by cyberthreats, internal attacks are initiated. External cyberattacks are started by third parties outside of the dominant network. IDS [33] primarily consists of three general components: observation, analysis, and detection. The Observation module collects data of the patterns, resources, and traffic on the network. The main components of IDS are typically analysis and detection of the traffic data using ML or DL algorithms. Based on predetermined algorithm, they can identify

intrusions. When an intrusion is discovered, the alert module raises attack flags [33]. This study has covered the following topics: security threats, detection method, IDS placement strategy, validation approach and datasets. This is because developing IDSs for IoT devices raises a significant challenge for data security researchers. Figure ٣ shows the brief taxonomy of the survey

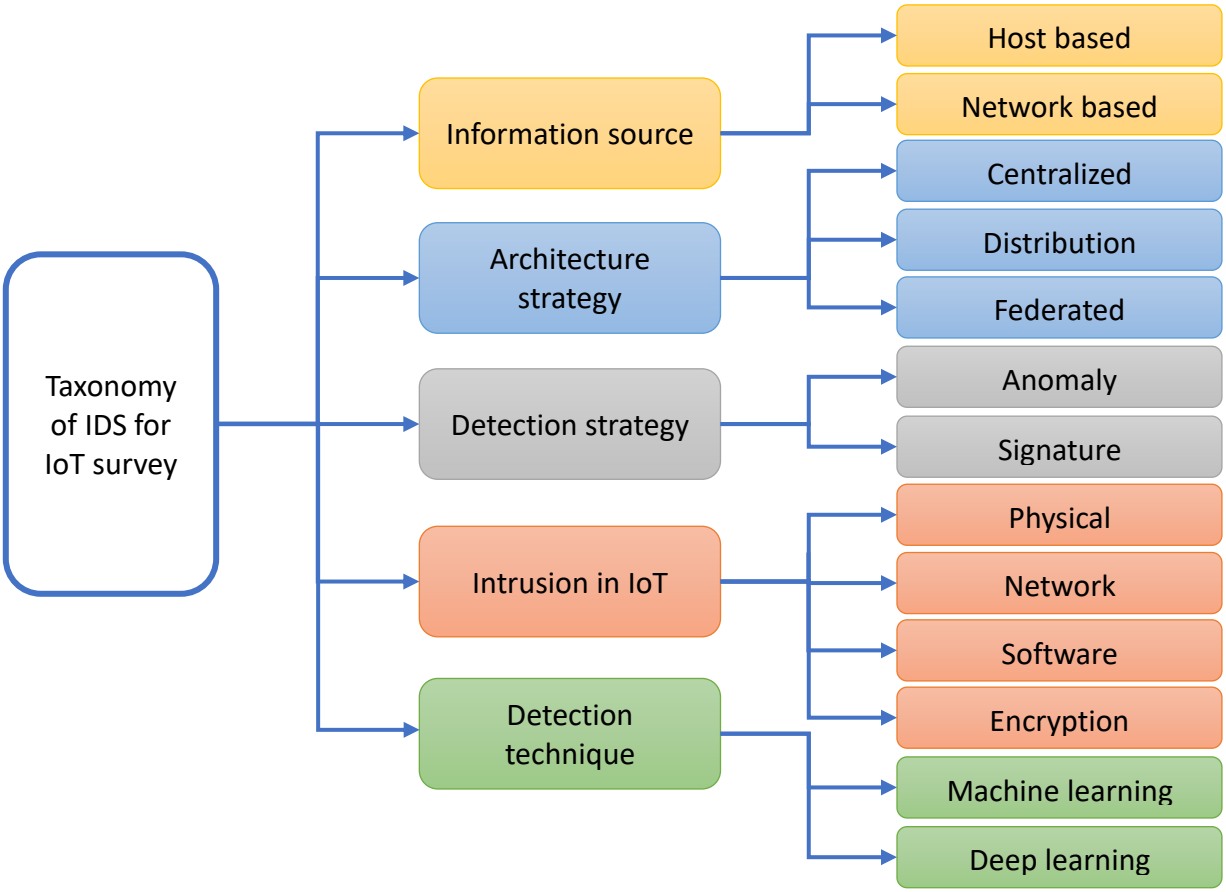

Figure 3: Taxonomy of IDS

4. IDS According to The Detection Strategies

However, a detailed analysis at the cyberattack on the IoT system reveals that there is always a behavioral pattern in the attacks [34], which can be discovered when ML and edge as well as cloud computing are combined to better build IDS. This section provided a detailed analysis of the many categories of IDS used in IoT networks. Researchers have included the conventional methodologies to develop ML based IDS and proposed several models. We divided IDS into Signature, Anomaly based categories [35] based on the framework, implementation, and operation.

4.1. Signature-Based NIDS in IoT Systems

This method detects attack patterns based on the presence of its signature in the system. However, this method is unable to detect new malware attacks whose signatures are absent from the list. Large datasets are frequently needed for signature-based NIDS in order to build reliable detection systems for IoT. The resources of IoT devices must be taken into account when restructuring traditional signature-based NIDS. There have been numerous attempts to create signature-based NIDS for IoT devices. A signature-based NIDS framework was proposed by Kasinathan et al. [36]. Their technology recognizes DoS attacks in networks based on 6LoWPAN [37]. To test their suggested methodology, the authors used Suricata, an open-source signature-based NIDS software [38]. Suricata, which does not explicitly target IoT networks, was created to detect infiltration in generic computer networks. Furthermore, there was no conclusive proof of Suricata's influence on the use of IoT devices in their investigation. The authors provided many methods for creating NIDS to safeguard the environment in [39-42]. the authors discussed various IDS design approaches for protecting IoT devices. The authors developed signature-based IDS using ML techniques to identify network intrusions in IoT devices. The authors used deep reinforcement learning to develop NIDS for industrial IoT in [43,44]. This method combines deep learning's observational powers with

reinforcement learning's decision-making capabilities to enable the efficient detection of various cyberattacks on the Industrial Internet of Things. Although the experimental findings in each of the research papers are encouraging, the authors were unable to show how their approach will work in an actual IoT network scenario.

4.2. Anomaly-Based NIDS for IoT Systems

This method is used by organizations to identify malwares, for which identification is difficult using the signature-based detection method. In this method, ML is used to create an activity model [45].

This method is effective at discovering new IoT system attacks. Particularly, those attacks initiated the misuse of the resources of IoT devices. A number of IDS created to protect IoT devices use anomaly-based techniques since they may be modelled to be lightweight. The authors of deployed ANN to identify intrusion in the gateway of the IoT system in [46-49]. To find anomalies in the data sent from the edge devices, they used ANN. The gateway was a high-resource network device that the researchers linked along with several IoT devices. Their outcomes were encouraging. The authors of [50–52] presented an IDS algorithm that leverages anomaly detection systems based on several ML techniques to identify threats in IoT systems. An IoT network attack often leaves its impact on the system, according to the authors. The authors suggested three methods, using this method to find these anomalies in their network. They did not, however, show any experimental evidence of false-positive rates, which is a significant issue with anomaly-based IDS. The authors also conducted a new investigation into how much memory and power Internet of Things devices need. The authors of [53,54] presented a smart home IDS that adapts autonomously to changing circumstances in the smart home by modifying the decision function of its underlying anomaly classification models. The research studies in this subsection show that anomaly-based IDS frequently begin by creating a baseline of the network's typical activity and traffic. Although they can be scaled down to be lightweight, anomaly-based NIDS are suitable for IoT systems

5. IDS According to The Information Source

The mode of operation of IDS designs for IoT can also be used to categorize them. The two primary modes in which NIDS operate are host-based and network-based.

5.1. Host-Based IDS for IoT Systems (HIDS)

HIDS is installed on independent networked devices by organizations. This system detects the organization traffic and alerts the administrator if any suspicious activities occur. One attribute of HIDS is that file systems storing the network analytical are protected from misplacements or changes and then an alert is sent to the administrator [55]. An IoT HIDS that can identify cyberattacks was created by Wang et al. [56]. The authors used experimental evidence to show that mimicking attacks do exist and that their prevention is necessary. The authors of [57] suggest a HIDS that was developed and designed to protect IoT devices, which form the core of IoT networks. Their method involves a group of suggested IDS that carry out conventional security verification and interact with HIDS controller to enable the coordination of intrusion detection actions in response to IoT devices targeted by DDoS attacks across the network.

5.2. Network-Based IDS for IoT Systems (NIDS)

NIDS monitors device traffic of the entire network, examines this traffic, and thereafter verifies the data against the packet metadata and content. An alert is sent to the network administrator if intrusions in the network are detected. One attribute of NIDS is the presence of a protecting firewall, owing to the system being installed at the same location [55]. NIDS, according to the authors [58], needed a lot of data in order to make intelligent decisions. The differences between host-based and network-based NIDS are shown in Table 3.

6. Datasets for IDS Design in IoT Systems

An ML-based IDS design must include the dataset. It consists of features identified during both normal and anomalous functioning of the targeted systems. Innovative techniques and detection algorithms for IoT networks required a preplanned dataset. Network packet extraction flows, system logs, and sessions are the three most typical data creation sources for IDS for IoT. It can be challenging and time-consuming to create a dataset specifically for IoT IDS. An overview of a number of popular public datasets utilized by the scientific community for IDS design can be found in Table 2.

The majority of researchers decide to build their own datasets for the ML-based IDS training. Regardless of how challenging it is to create a dataset, it is necessary to evaluate and compare models using a widely used benchmark dataset. To train IDS, researchers used numerous datasets. **The KDD-Cup'99** [59], which was made for the KDD competition and comprises 41 features similar to a NetFlow dataset, is one of the most often cited datasets in the literature. The Canadian Institute of Cybersecurity produced the **UNB-ISCX 2012** [60], **CICIDS 2017 [61], and AWS (CSE-CIC-IDS 2018)** [62] datasets. The dataset, according to the authors [63], was built using data from five days of both normal and attack traffic. The majority of the essential modern and updated attack criteria, including DoS, DDoS, Brute Force, XSS, SQL Injection, Infiltration, Port scan, and Botnet, are present in the CICIDS2017. Eighty features were retrieved from the dataset using the flow meter [64]. **The UNSW NB15,** which was produced by the defense force academy of University of New South Wales Australia, is another popular dataset

that is now being utilized as a benchmark for IDS in IoT [65, 66]. Through realistic network operations, the UNSW NB15 was developed based on the most recent attack categories. Ten (10) different types of attacks are included in the UNSW NB15 dataset: analysis, backdoor, denial-of-service, exploit, fizzers, generic, reconnaissance, shellcode, and worm. There are already a number of open-source datasets that focus on various IoT cyberattacks. The authors of [67] simulated several network threats in an IoT scenario. Their dataset includes the Mirai Botnet, benign, mitm-arpspoofing, DoS-synflooding, scan-hostport, and scan portos. **IoTID20** is a dataset developed by Ullah et al. [68] for the IoT IDS. The IoT botnet dataset, which is appropriate for DoS attacks, was suggested by the authors. IoT/IIoT service telemetry, Operating System logs, and IoT network traffic were all acquired from a realistic approximation of a medium-scale network at the UNSW Canberra Cyber Range and IoT Labs, according to a new dataset named **TON IoT** proposed by Moustafa [69]. A CPPS testbed based on OPC UA was used to develop and inject a number of attacks to produce the **OPCUA dataset** [70], which enables users to evaluate the effectiveness of different IDS building techniques in an industrial environment. About IDS in IoT systems is addressed in details in Table 6. Anomalies in industrial IoT are detected using datasets like the **ELEGANT dataset** [71-73], which targets DoS/DDoS attack in IoT and SDN-based IoT networks. The MQTT protocol IoT network's **MQTT-iot-ids2020 dataset** [74] detects network intrusion. In order to identify DoS/DDoS attacks, information gathering, Man in the Middle attacks, Injection attacks, and Malware attacks, the **Edge-IIoTset dataset** [75] was also developed for industrial IoT. The **IoT-BDA Botnet Analysis Dataset** [76], which was developed to make it simpler to develop host and network-based IDS, is the last dataset on the IDS IoT system radar. For researchers to create reliable IDS to secure the IoT system, all of the aforementioned datasets are openly available.

Table 2: Popular public datasets for IDS

Dataset name	Year	Categories
CSE-CIC-IDS2018 [62]	2018	DoS DDoS Brute Force XSS SQL Injection Infiltration Portscan Botnet
TON_IoT Dataset [68]	2019	DoS DDoS ransomware
THE BOT-IOT DATASET [77]	2019	Normal DDoS DoS OS Fingerprinting Service Scan Keylogging Data Theft
Mqtt-iot-ids2020 DATASET [71]	2020	Normal aggressive scan UDP scan Sparta SSH brute-force MQTT brute-force attack.
OPCUA dataset [70]	2020	DoS Eavesdropping Man-in-the-middle, Impersonation Spoofing attacks
IOT-BDA BOTNET ANALYSIS DATASET [76]	2021	Port scanning Exploitation C2 communications DDoS
X-IIoTID dataset [78]	2021	Brute force attack dictionary attack

		the malicious insider reverse shell Man-in-the-Middle
Edge-IIoTset DATASET [75]	2022	DoS DDoS attacks Information gathering Man in the middle attacks, Injection attacks Malware attacks

7. IDS According to The Architecture Strategy

We also classify the IDS according to how they are deployed, as shown in Figure 4. This type of IDS is relying on the placement, position, and part of the system where it is located. The placement strategies for IDS in IoT systems are discussed in this subsection.

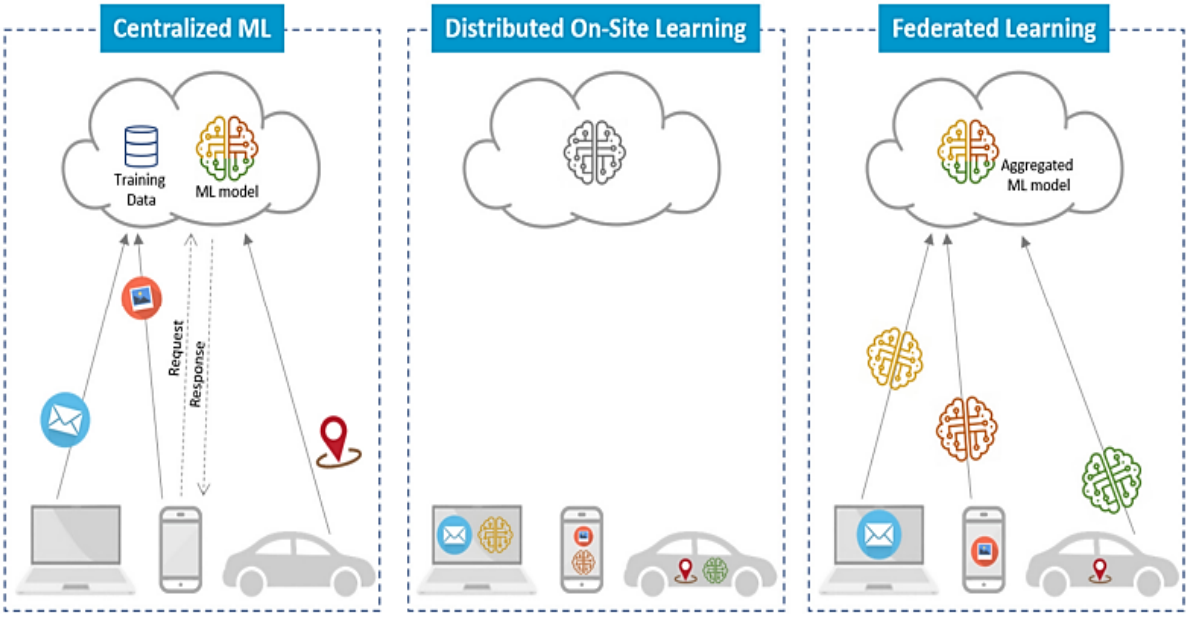

Figure 4: IDS architecture strategies

7.1. Centralized Placement IDS for IoT Systems

ML model is built in the cloud. Sending data to the cloud server; the user uses the model using API; sending request in order to access the service. IDS examines all the traffic from the connected IoT devices that enters and exits the border router in the centralized manner. The centralized deployment approach has the drawback of failing to detect attacks on internal IoT networks. The centralized placement strategy was employed by the authors of [36] to implement their suggested IDS. Their research concentrated on mitigating DoS attacks against IoT systems. In order to detect and analyze network data, they needed a dedicated host. They used a wired network connection to link the host IDS while using wireless connections for the other IoT devices. In the case that the network is hacked, the method aids the IDS in detecting the DoS attacks. A border router-based centralized IDS was the idea proposed by Wallgren et al. [79]. Their primary objective was to find IoT network threats. The authors suggested an IoT heartbeat protocol that would send ICMPv6 echo requests to all border routers and other IoT devices network to identify intrusions. Additionally, Jun et al. [80] proposed Complex Event-Processing. (CEP) solutions for IoT system network intrusion detection. The writers used an organized strategy and installed the NIDS in the border router to keep an eye on the network traffics. Utilizing event features is the suggested system's primary benefit. In addition, some researchers have studied the attack detection algorithms based on ML algorithms and DL neural networks for IoT systems as shown in Table 3.

Table 3: Study on ML algorithms and DL neural networks for IoT systems

Research	Model	Classification type	Shortcomings
Fatani, et al. 2021 [81]	CNN-TSODE	Binary Multi	Sending training data to central model leads to the inefficiency of bandwidth and energy concerns
Ferrag, et al. 2020 [82]	DNN RNN CNN	Multi	High communication overhead associated with sending raw data to the central node
Ferrag, et al. 2019 [83]	RNN	Multi	Increasing network scale decreases the performance
Aldhaheri, et al. 2020 [84]	DeepDCA (DCA-SNN)	Binary	Single point of failure affects QoS
Pokhrel, et al. 2021 [85]	NB KNN ANN	Binary	High costs of gathering data to central node over the 5G/6G network
Kumar, et al. 2021 [86]	RF XG Boost	Multi	Transferring of personal data to centralized entity affects the privacy
Hussain, et al. 2021 [87]	NB KNN RF Log R DT	Binary	Collecting sensitive data of end users raises privacy preservation concerns
Shafiq, et al. 2020 [88]	DT NB RF SVM	Multi	Model is time consuming due to centralized processing

7.2. Distributed Placement IDS for IoT Systems

The Cloud distributes the local model to each device; local models with local datasets; connection to the cloud no longer needed [89]. The IDSs are distributed across the network's numerous IoT devices under the decentralized placement method. Each system must be configured separately, and the NIDS must be lightweight due to the resource limitations of the IoT system. Lightweight DL models have been developed for edge computing. To classify benign traffic from distributed denial of service (DDoS) attacks, Roberto et al. [90] proposed LUCID, a lightweight IDS that is based on CNNs and exhibits excellent pattern-recognition ability. Latif et al. [91] presented a novel lightweight random neural network (RaNN) for prediction of attacks such as DoS, malicious operation, malicious control, data type probing, spying, and scans. The RaNN is compared with the traditional ANN, SVM, and DT and achieves higher attack detection accuracy (by an average of 5.65%) than the other algorithms. Watchdogs are Internet of Things (IoT) devices that are set up to monitor vulnerabilities in local linked devices. This positioning technique was applied by Cernantes et al. [92] in their research.

The watchdog was employed by the INTI to identify and stop attacks. In their experiment, an IoT device was selected as the head node or the leader of the network clusters. Due to the network reconfiguration policy that connected IoT devices introduced, each device's function may vary over time. An IoT device broadcasts a message to other devices whenever it notices an intrusion to protect them. The IDSs are distributed among the numerous IoT devices under the decentralized placement strategy. A distributed and lightweight NIDS built on an Artificial Immune System was created by Farhoud et al (AIS). They dispersed their AIS amongst IoT, the edge, and the cloud. A distributed NIDS that detected attacks was created by the authors in [93], with such a part of the detection model hosted on an IoT device and the residual model hosted on ISP resources (ISP). They created the IDS to protect house gateway systems that link Internet-connected smart home IoT gadgets to one another. An IDS system created and tested by Zeeshan et al. [94] is best suited for small IoT devices. They applied a process for managing trust that enables IoT devices to handle crucial data about connected neighbors. The IoT device can distinguish harmful patterns in the network thanks to this method. [95] suggested an IDS that makes use of information flow processing to collect event data from distributed sources as soon as significant data is received. Additionally, their technology was capable of real-time intrusion detection. In order to detect intrusions, a collaborative NIDS was suggested in [96] by distributing the IDS model among the numerous IoT devices. By splitting the expense of monitoring the IDS across the IoT devices, the amount of energy, processing capability, and storage capacity needed for the detection was reduced. Furthermore, Brik et al. [97] applied the features of FL to UAV-enabled wireless networks led to a decrease in the communication overhead while maintaining the data privacy in a distributed manner.

2.2. Federated Placement IDS for IoT Systems

Some distributed systems have a centralized IDS that supervises the other security systems placed in other IoT systems in the same network [98]. McMahan et al. [99] (the Google team) presented an alternative technique to centralized learning of deep networks. This technique involved leaving the data of the training distributed on the mobile devices, locally training mobile models, aggregating locally computed updates to the server, learning global models, and broadcasting learning updates to local models. They referred to this approach as “Federated Learning.” This method preserves the privacy of the local trained data, which is necessary for various fields. Nguyen et al. [100] presented (DÏoT) an anomaly detection for IoT systems based on a self-learning federated distributed system, Gated Recurrent Unit (GRU), a type of RNN. DÏoT was the first algorithm that employed the federated learning approach in detecting intrusions. The results revealed the high accuracy and rapid detection rate of DÏoT (95.6% and 257 ms). However, low end devices are problematic, owing to the long training time of GRU. Wang et al. [101] developed an algorithm which, compared with DÏoT, is better suited for these devices by adjusting the FL algorithm. A multitask deep neural network in federated learning (MT-DNN-FL) has also been proposed by Zhao et al. [102]. The CICIDS2017, ISCXVPN2016, and ISCXT datasets were used in the performance evaluation of this algorithm. The results revealed that the proposed algorithm has a good detection rate with respect to the multitasks and reduces the training time compared with that of centralized training. However, optimization of the DNN structure is required in order for the proposed model to cope with restrictions of IoT devices. Chatterjee et al. [103] proposes a Probabilistic Hybrid Ensemble Classification (PHEC) model in the centralized and federated mode The study revealed that, compared with these modes, the FL mode performs better regarding privacy issues of the data and the problem of data processing in a single system. Man et al. [104], presented a FEDACNN model based on CNN to solve the communication delay issue in the system by reducing communication rounds to 50%. Rajendran et al [105] proposed two FL models with ANN and LR for patient data privacy and security in healthcare systems. Due to the lower complexity of LR (compared with that of other methods) and lack of epochs, FL will yield no improvement in the performance of the model. Compared with ANN models, FL yields better accuracy

and privacy. Chen et al. [106] presented a Federated Learning-based Attention Gated Recurrent Unit (FedAGRU) algorithm for securing wireless edge networks with intrusion detection. Furthermore, the study also proposed a mechanism for avoiding the upload of unimportant data to the cloud and increasing the weight of important devices in order to decrease communication overhead. The results showed that the proposed FedAGRU algorithm enhanced the accuracy by ~8% and reduced costs by70%, respectively, compared with centralized systems and other FL algorithms. Rieke et al. [107] discussed the impact of FL on the future of digital healthcare by considering the issues regarding medical sensitive data privacy, which can be achieved without exchanging or centralizing data sets. However, the corresponding security issues remain unexplored.

8. IoT-based IDS with ML/ DL and Evaluation Metrics

The metrics and benchmark datasets, as well as some of the common ML methods, are the main topics of this section of the survey. Real-time data from the network of the installed devices, rather than modelling or simulation, is the best way to evaluate any IDS. Other classification models may view data packets that some ML-based IDS algorithm classifies as an intrusion in a network as valid. To evaluate IDS, researchers employ a variety of metrics. No one indicator appears to be sufficient to examine the performance and efficiency of IDS. According to [108], the Detection Rate (DR) and False Alarm Rate (FAR). of an IDS can be used to assess its performance According to all of the aforementioned evaluations, the performance of the IDS created for an IoT use case may varies. The type of metrics depends on the implementation procedure, the attack type, the resource of the IoT device, and the machine learning applied during the IDS.

However, accuracy, recall/sensitivity, and F1-Score are the metrics that researchers employ the most frequently. The effectiveness of an IDS for IoT systems is evaluated using metrics like false negative rate (FNR), and false positive rate (FPR), as shown in Table 4.

Table 4: Evaluation metrics for IDS

Metric	Equation	Definition
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$	Ratio of correctly predicted instances to total number of predicted instances.
Precision (Detection rate)	$\frac{TP}{TP+FP}$	Ratio of the correctly predicted positive instances to total positive predictions.
Recall (Sensitivity)	$\frac{TP}{TP+FN}$	Ratio of the correctly predicted positive instances to the overall available positive data category.
Specificity	$\frac{TN}{TN+FP}$	Ratio of the correctly predicted negative instances to the overall available negative data category.
F1-score	$\frac{2TP}{2TP+FP+FN}$	Hybrid metric indicates the overall performance of the model respecting to Both precision and recall, useful for unbalanced classes
False alarm rate	$\frac{FP}{FN+FP}$	Ratio of false positive alarms per the total number of false prediction warnings or alarms.

No matter how long NIDS have been in development, they still have trouble improving detection accuracy, reducing overall on false alarms, and identifying newly developed attacks. Modern researchers concentrated on creating IDS that make use of ML techniques in order to solve the aforementioned issues. With great accuracy, ML algorithms automatically detect the distinctive features in abnormal data present inside normal data. Additionally, because ML algorithms have significant generalization potentials, they can recognize unidentified attacks [109]. ML-based NIDS are intended to monitor the host and its settings, examine the behavior of the systems, produce alerts, and react to any suspected attacks [110]. K-NN and Naive Bayes were employed by the authors of [111] to detect intrusion. The NSL-KDD dataset was used to test their model. In [112,113], the authors suggested a logistic

regression-based IDS model (BOTNET) for IoT device intrusion detection. Researchers have developed IDS for IoT systems using ML techniques as Decision Tree [114], K-Mean [115], DNN (using the NSL-KDD dataset) [116], and CNN (using the NGIDS-DS and ADFA-LD dataset for benchmark) [117]. The most popular neural network ML-based techniques employed by the research community to develop IDS for IoT include RNN, LSTM, GRU, and GAN [118,119]. Table 5 shows the state of the art of the ML based IDS.

Table 5: Comparative study on the ML based IDS.

Ref	Model	Classification type	Accuracy	Precision (detection rate)	Recall	F1-score	Mode	Integration with blockchain
Fatani, A.; et al. [81]	CNN-TSODE	Binary	99.99%	99.99%	99.99%	99.99%	Centralized	No
		Multi	99.04%	99.04%	99.04%	99.04%		
Ferrag, M.A.; et al. [82]	DNN	Multi	98.37%	---	---	---	Centralized	No
	RNN							
	CNN							
Ferrag, M.A.; Maglaras, L. [83]	RNN	Multi	98.20%	-----	---	---	Centralized	No
Aldhaheri, S.; et al. [84]	DeepDCA (DCA-SNN)	Binary	98.73%	99.17%	98.36%	98.77%	Centralized	No
Pokhrel, S.; Abbas, R.; Aryal, B. [85]	Naive Bayes	Binary	51.5%	---	---	---	Centralized	No
	KNN		92.1%	---	---	---		
	ANN		82.8%	---	---	---		
Kumar, P.; et al. [86]	RF	Multi	99.99%	99.99%	99.99%	99.99%	Centralized	Yes
	XGBoost		99.99%	87.77%	94.36%	87.90%		

Hussain, F.; et al. [87]	NB	Binary	52.18%	79.67%	99.70%	69.50%	Centralized	No
	KNN		99.48%	99.65%	99.68%	99.58%		
	RF		99.51%	99.70%	99.79%	99.65%		
	Log R		99.50%	95.28%	90.39%	94.70%		
	DT		99.47%	99.69%	99.79%	99.63%		
Shafiq, M.; et al. [88]	decision tree	Multi	99.99%	97.10%	94.27%	98.95%	Centralized	No
	Naive Bayes		97.49%	56.28%	57.95%	98.44%		
	Random Forest		99.98%	95.05%	91.37%	99.99%		
	SVM		97.80%	57.89%	43.24%	98.48%		
Huong, T.T.; et al. [120]	ANN	Multi	99.9%	---	---	---	Centralized	No
			92.5%	---	---	---	Federated	
Preuveneers et al. [121]	Auto-encoder	Binary	97%	---	---	---	Distributed	Yes
Roberto et al. [90]	LUCID	Binary	98.88%	---	---	98.89%	Distributed	No
Latif et al. [91]	RaNN	Binary	99.2%	99.11%	99.13%	99.20%	Distributed	No
Nguyen et al. [100]	GRU	Binary	95.6%	---	---	---	Federated	No
Man et al. [104]	CNN	Multi	99.76%	---	---	---	Federated	No

Rajendran et al [105]	ANN LR	Binary	73.52% 74.02%	---	35.03% 71.48%	---	Federated	No
Chen et al. [106]	GRU-SVM	Binary	99.28%	---	---	98.12%	Federated	No
Ashraf E. et al. [122]	ANN	Binary	99.99%	100%	99.99%	99.99%	Federated	Yes

Conclusion

The demand to secure IoT systems has generated a variety of creative IDS design solutions. This paper has undertaken a thorough analysis of IDS that makes use of ML, DL, edge and cloud computing. There was an illustration of a taxonomy and tabular classification of validation techniques, IDS placement schemes, security threats, and detection techniques. We have found that there is a significant number of scientific frameworks. The evolution of IDS in the real world hasn't been experimentally verified yet, though. There aren't any specified standards for certain detection strategies or deployment methodologies to protect IoT systems. Designing a realistic NIDS solution that successfully identifies cyber-attacks in realistic IoT systems still needs more work. Additionally, most IoT system evaluation methods do not take consideration important metrics like energy usage, processing, and storage efficiency in most of the studies. We have found numerous interesting study directions through our careful review. First and foremost, future IDS for IoT systems should concentrate on enhancing IDS effectiveness; and illustrate how their proposed systems could be implemented in existing IoT infrastructure. We are optimistic that this survey will be helpful to researchers in creating IDS for IoT systems as resources and guidelines.

Disclosure

The author reports no conflicts of interest in this work.

Tables and graphs

References

1. Li, H.; Ota, K.; Dong, M. Learning IoT in edge: Deep learning for the Internet of Things with edge computing. IEEE Netw. 2018, 32, 96–101.

2. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 2020, 22, 1191–1221.

3. Yastrebova, A.; Kirichek, R.; Koucheryavy, Y.; Borodin, A.; Koucheryavy, A. Future networks 2030: Architecture & requirements. In Proceedings of the 2018 10th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Moscow, Russia, 5–9 November 2018; pp. 1–8.

4. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.A. Security considerations for Internet of Things: A survey. SN Comput. Sci. 2020, 1, 1–19.

5. Shi, W.; Dustdar, S. The promise of edge computing. Computer 2016, 49, 78–81. [CrossRef]

6. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. IEEE Internet Things J. 2016, 3, 637–646.

7. Ranaweera, P.; Jurcut, A.D.; Liyanage, M. Survey on multi-access edge computing security and privacy. IEEE Commun. Surv. Tutor. 2021, 23, 1078–1124.

8. Pacheco, J.; Hariri, S. IoT security framework for smart cyber infrastructures. In Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), Augsburg, Germany, 12–16 September 2016; pp. 242–247.

9. Borhani, M.; Liyanage, M.; Sodhro, A.H.; Kumar, P.; Jurcut, A.D.; Gurtov, A. Secure and resilient communications in the industrial internet. In Guide to Disaster-Resilient Communication Networks; Springer: Berlin/Heidelberg, Germany, 2020; pp. 219–242.

10. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf. Secur. Appl. 2018, 38, 8–27.

11. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. 2017, 4, 1250–1258.

12. Sain, M.; Kang, Y.J.; Lee, H.J. Survey on security in Internet of Things: State of the art and challenges. In Proceedings of the 2017 19th International conference on advanced communication technology (ICACT), Pyeongchang, Korea, 19–22 February 2017; pp. 699–704.

13. Benabdessalem, R.; Hamdi, M.; Kim, T.H. A survey on security models, techniques, and tools for the internet of things. In Proceedings of the 2014 7th International Conference on Advanced Software Engineering and Its Applications, Hainan Island, China, 20–23 December 2014; pp. 44–48.

14. Jurcut, A.D.; Ranaweera, P.; Xu, L. Introduction to IoT security. In IoT Security: Advances in Authentication; John Wiley & Sons: Hoboken, NJ, USA, 2020; pp. 27–64.

15. Khan, B.U.I.; Olanrewaju, R.F.; Anwar, F.; Mir, R.N.; Najeeb, A.R. A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem. Int. J. Inf. Comput. Secur. 2019, 11, 332–354.

16. Pongle, P.; Chavan, G. A survey: Attacks on RPL and 6LoWPAN in IoT. In Proceedings of the 2015 International conference on pervasive computing (ICPC), Pune, India 8–10 January 2015; pp. 1–6.

17. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. 2015, 2, 515–526.

18. Wang, H.; Zhang, Z.; Taleb, T. Special issue on security and privacy of IoT. World Wide Web 2018, 21, 1–6.

19. Aldabbas, H.; Amin, R. A novel mechanism to handle address spoofing attacks in SDN based IoT. Clust. Comput. 2021, 24, 3011–3026.

20. Ferrag, M.A.; Shu, L.; Djallel, H.; Choo, K.K.R. Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0. Electronics 2021, 10, 1257.

21. Gupta, B.; Chaudhary, P.; Chang, X.; Nedjah, N. Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. Comput. Electr. Eng. 2022, 98, 107726.

22. Alyas, M.; Noor, M.I.; Hassan, H. DDOS Attack Detection Strategies in Cloud A Comparative Stud. VFAST Trans. Softw. Eng. 2017, 12, 35–42.

23. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. Computer 2017, 50, 80–84.

24. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F.R. A multi-level DDoS mitigation framework for the industrial internet of things. IEEE Commun. Mag. 2018, 56, 30–36.

25. Abdalzaher, M.S.; Elwekeil, M.; Wang, T.; Zhang, S. A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio. IEEE Syst. J. 2021.

26. Kerrakchou, I.; Chadli, S.; Kharbach, A.; Saber, M. Simulation and Analysis of Jamming Attack in IoT Networks. In Proceedings of the International Conference on Digital Technologies and Applications, Moscow, Russia, 30–31 March 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 323–333.

27. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle Attack Mitigation in Internet of Medical Things. IEEE Trans. Ind. Inform. 2021, 18, 2053–2062.

28. Pospisil, O.; Fujdiak, R.; Mikhaylov, K.; Ruotsalainen, H.; Misurec, J. Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study. Appl. Sci. 2021, 11, 7642.

29. Kambourakis, G.; Kolias, C.; Stavrou, A. The mirai botnet and the iot zombie armies. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 267–272. Sensors 2022, 22, 3744 27 of 33

30. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baiot—Network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018, 17, 12.22.

31. Rajan, A.; Jithish, J.; Sankaran, S. Sybil attack in IOT: Modelling and defenses. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Chennai, India, 3–5 August 2017; pp. 2323–2327.

32. Evangelista, D.; Mezghani, F.; Nogueira, M.; Santos, A. Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination. In Proceedings of the 2016 Wireless Days (WD), Toulouse, France, 23–25 March 2016; pp. 1–6.

33. Alrajeh, N.A.; Khan, S.; Shams, B. Intrusion detection systems in wireless sensor networks: A review. Distrib. Sens. Netw. 2013, 9, 167575.

34. Vaca, F.D. An Ensemble Learning Based Multi-Level Network Intrusion Detection System for Wi-Fi Dominant Networks. Ph.D. Thesis, Purdue University Graduate School, Lafayette, IN, USA, 2019.

35. Abduvaliyev, A.; Pathan, A.S.K.; Zhou, J.; Roman, R.; Wong, W.C. On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. 2013, 15, 1223–1237.

36. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.

37. Olsson, J. 6LoWPAN demystified. Tex. Instrum. 2014, 13, 1–13.

38. Boujrad, M.; Lazaar, S.; Hassine, M. Performance Assessment of Open-Source IDS for improving IoT Architecture Security implemented on WBANs. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Msida, Malta, 15–17 December 2020; pp. 1–4.

39. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the Networks, Computers and Communications (ISNCC), Marrakech, Morocco, 16–18 May 2016; pp. 1–6.

40. Hanif, S.; Ilyas, T.; Zeeshan, M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; pp. 152–156.

41. Qureshi, A.U.H.; Larijani, H.; Ahmad, J.; Mtetwa, N. A heuristic intrusion detection system for Internet-of-Things (IoT). In Proceedings of the Intelligent Computing, Proceedings of the Computing Conference, London, UK, 16–17 July 2019; Springer: Berlin/Heidelberg, Germany. 2019; pp. 86–98.

42. Almogren, A.S. Intrusion detection in Edge-of-Things computing. J. Parallel Distrib. Comput. 2020, 137, 259–265.

43. Tharewal, S.; Ashfaque, M.W.; Banu, S.S.; Uma, P.; Hassen, S.M.; Shabaz, M. Intrusion detection system for industrial Internet of Things based on deep reinforcement learning. Wirel. Commun. Mob. Comput. 2022, 2022, 9023719.

44. Caminero, G.; Lopez-Martin, M.; Carro, B. Adversarial environment reinforcement learning algorithm for intrusion detection. Comput. Netw. 2019, 159, 96–109.

45. Aldabbas, H.; Amin, R. A novel mechanism to handle address spoofing attacks in SDN based IoT. Clust. Comput. 2021, 24, 3011–3026.

46. Canedo, J.; Skjellum, A. Using machine learning to secure IoT systems. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust, PST, Auckland, New Zealand, 12–14 December 2016; pp. 219–222.

47. Wu, Y.; Dai, H.N.; Tang, H. Graph neural networks for anomaly detection in industrial internet of things. IEEE Internet Things J. 2021.

48. Pacheco, J.; Benitez, V.H.; Felix-Herran, L.C.; Satam, P. Artificial neural networks-based intrusion detection system for internet of things fog nodes. IEEE Access 2020, 8, 73907–73918.

49. Alladi, T.; Agrawal, A.; Gera, B.; Chamola, V.; Sikdar, B.; Guizani, M. Deep neural networks for securing IoT enabled vehicular ad-hoc networks. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.

50. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet Things J. 2020, 7, 6882–6897.

51. Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. Appl. Sci. 2021, 11, 8383.

52. Kumar, P.; Gupta, G.P.; Tripathi, R. Design of anomaly-based intrusion detection system using fog computing for IoT network. Autom. Control Comput. Sci. 2021, 55, 137–147.

53. Heartfield, R.; Loukas, G.; Bezemskij, A.; Panaousis, E. Self-configurable cyber-physical intrusion detection for smart homes

using reinforcement learning. IEEE Trans. Inf. Forensics Secur. 2020, 16, 1720–1735.

54. Ma, X.; Shi, W. Aesmote: Adversarial reinforcement learning with smote for anomaly detection. IEEE Trans. Netw. Sci. Eng. 2020, 8, 943–956.

55. Salih, A.A. and A.M. Abdulazeez, *Evaluation of classification algorithms for intrusion detection system: A review.* Journal of Soft Computing and Data Mining, 2021. **2**(1): p. 31-40.

56. Wang, X.; Lu, X. A host-based anomaly detection framework using XGBoost and LSTM for IoT devices. Wirel. Commun. Mob. Comput. 2020, 2020, 8838571.

57. Kfouri, G.d.O.; Gonçalves, D.G.; Dutra, B.V.; de Alencastro, J.F.; de Caldas Filho, F.L.; e Martins, L.M.; Praciano, B.J.; de Oliveira Albuquerque, R.; de Sousa, R.T., Jr. Design of a distributed HIDS for IoT backbone components. Ann. Comput. Sci. Inf. Syst. 2019, 81–88.

58. Smys, S.; Basar, A.; Wang, H. Hybrid intrusion detection system for internet of things (IoT). J. ISMAC 2020, 2, 190–199.

59. Tsai, C.F.; Lin, C.Y. A triangle area based nearest neighbors approach to intrusion detection. Pattern Recognit. 2010, 43, 222–229.

60. IDS 2012 Datasets Research Canadian Institute for Cybersecurity UNB. Available online: https://www.unb.ca/cic/datasets/ids. html (accessed on 22 April 2020).

61. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the International Conference on Information Systems Security and Privacy, Funchal, Madeira, 22–24 January 2018; pp. 108–116. Available online: https://www.scitepress.org/Papers/2018/66398/66398.pdf (accessed on 17 October 2021).

62. IDS 2018 Datasets Research Canadian Institute for Cybersecurity UNB. Available online: https://www.unb.ca/cic/datasets/ids2018.html (accessed on 22 April 2020).

63. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the International Conference on Information Systems Security

64. Ullah, I.; Mahmoud, Q.H. A two-level hybrid model for anomalous activity detection in IoT networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–6.

65. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6.

66. Moustafa, N.; Slay, J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Inf. Secur. J. Glob. Perspect. 2016, 25, 18–31. [CrossRef]

67. Kang, H.; Ahn, D.H.; Lee, G.M.; Yoo, J.; Park, K.H.; Kim, H.K. IoT Network Intrusion Dataset. IEEE Dataport. 2019. Available online: https://ieee-dataport.org/ieee-dataport-dataset-upload-contest-entries (accessed on 10 January 2022).

68. Ullah, I.; Mahmoud, Q.H. A scheme for generating a dataset for anomalous activity detection in iot networks. In Proceedings of the Canadian Conference on Artificial Intelligence, Ottawa, ON, Canada, 13–15 May 2020; Springer: Berlin/Heidelberg, Germany, 2020, pp. 508–520.

69. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access 2020, 8, 165130–165150. [CrossRef]

70. Pinto, R.; Gonçalves, G.; Tovar, E.; Delsing, J. Attack detection in cyber-physical production systems using the deterministic dendritic cell algorithm. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020; Volume 1, pp. 1552–1559

71. Sousa, B.; Cruz, T.; Arieiro, M.; Pereira, V. An ELEGANT dataset with Denial of Service and Man in The Middle attacks. arXiv 2021, arXiv:2103.09380.

72. Sambangi, S.; Gondi, L.; Aljawarneh, S.; Annaluri, S.R. SDN DDOS Attack Image Dataset. 2021. Available online: https://ieee-dataport.org/documents/sdn-ddos-attack-image-dataset (accessed on 10 January 2022)

73. Hussain, F.; Abbas, S.G.; Husnain, M.; Fayyaz, U.U.; Shahzad, F.; Shah, G.A. IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6.

74. Hindy, H.; Tachtatzis, C.; Atkinson, R.; Bayne, E.; Bellekens, X. Mqtt-iot-ids2020: Mqtt Internet of Things Intrusion Detection Dataset. IEEE Dataport. 2020. Available online: https://ieee-dataport.org/open-access/mqtt-iot-ids2020-mqtt-internet-thingsintrusion-detection-dataset (accessed on 11 January 2022)

75. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access 2022, 40281–40306.

76. Trajanovski, T.; Zhang, N. IoT-BDA Botnet Analysis Dataset. IEEE Internet Things J. 2021, 9.

77. Moustafa, N. The Bot-IoT Dataset. 2019. Available online: https://ieee-dataport.org/documents/bot-iot-dataset (accessed on 11 January 2022

78. Al-Hawawreh, M.; Sitnikova, E.; Aboutorab, N. X-IIoTID: A connectivity-and device-agnostic intrusion dataset for industrial Internet of Things. IEEE Internet Things J. 2021, 9, 3962–397.

79. Wallgren, L.; Raza, S.; Voigt, T. Routing Attacks and Countermeasures in the RPL-based Internet of Things. Int. J. Distrib. Sens. Netw. 2013, 9, 794326.

80. Jun, C.; Chi, C. Design of complex event-processing IDS in internet of things. In Proceedings of the 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, Zhangjiajie, China, 10–11 January 2014; pp. 226–229.

81. Fatani, A., et al., IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access, 2021. 9: p. 123448-123464.

82. Ferrag, M.A., et al., Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 2020. 50: p. 102419.

83. Ferrag, M.A. and L. Maglaras, DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Transactions on Engineering Management, 2019. 67(4): p. 1285-1297.

84. Aldhaheri, S., et al., Deepdca: novel network-based detection of iot attacks using artificial immune system. Applied Sciences, 2020. 10(6): p. 1909.

85. Pokhrel, S., R. Abbas, and B. Aryal, IoT security: botnet detection in IoT using machine learning. arXiv preprint arXiv:2104.02231, 2021.

86. Kumar, P., et al., A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. Transactions on Emerging Telecommunications Technologies, 2021. 32(6): p. e4112.

87. Hussain, F., et al., A framework for malicious traffic detection in IoT healthcare environment. Sensors, 2021. 21(9): p. 3025.

88. Shafiq, M., et al., CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet of Things Journal, 2020. 8(5): p. 3242-3254.

89. Pospisil, O.; Fujdiak, R.; Mikhaylov, K.; Ruotsalainen, H.; Misurec, J. Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study. Appl. Sci. 2021, 11, 7642.

90. Doriguzzi-Corin, R., et al., LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 2020. 17(2): p. 876-889.

91. Latif, S., et al., A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access, 2020. 8: p. 89337-89350.

92. Cervantes, C.; Poplade, D.; Nogueira, M.; Santos, A. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015 pp. 606–611.

93. Gajewski, M.; Batalla, J.M.; Mastorakis, G.; Mavromoustakis, C.X. A distributed IDS architecture model for Smart Home systems. Clust. Comput. 2019, 22, 1739–1749.

94. Khan, Z.A.; Herrmann, P. A trust based distributed intrusion detection mechanism for internet of things. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 1169–1176.

95. Zhou, C.V.; Leckie, C.; Karunasekera, S. A survey of coordinated attacks and collaborative intrusion detection. Comput. Secur. 2010, 29, 124–140.

96. Arshad, J.; Azad, M.A.; Abdellatif, M.M.; Rehman, M.H.U.; Salah, K. COLIDE: A collaborative intrusion detection framework for Internet of Things. IET Netw. 2018, 8, 3–14.

97. Brik, B., A. Ksentini, and M. Bouaziz, *Federated learning for UAVs-enabled wireless networks: Use cases, challenges, and open problems* .IEEE Access, 2020. **8**: p. 53841-53849

98. Abraham, A.; Thomas, J. Distributed intrusion detection systems: A computational intelligence approach. In Applications of Information Systems to Homeland Security and Defense; IGI Global: Hershey, PA, USA, 2006; pp. 107–137.

99. McMahan, H.B., et al., Federated learning of deep networks using model averaging. arXiv preprint arXiv:1602.05629, 2016. 2.

100. Nguyen, T.D., et al. DÏoT: A federated self-learning anomaly detection system for IoT. in 2019 IEEE 39th International conference on distributed computing systems (ICDCS). 2019. IEEE.

101. Wang, S., et al., *Adaptive federated learning in resource constrained edge computing systems.* IEEE Journal on Selected Areas in Communications, 2019. **37**(6): p. 1205-1221.

102. Zhao, Y., et al. multi-task network anomaly detection using federated learning. in Proceedings of the tenth international symposium on information and communication technology. 2019.

103. Chatterjee, S. and M.K. Hanawal, Federated learning for intrusion detection in IoT security: a hybrid ensemble approach. arXiv preprint arXiv:2106.15349, 2021.

104. Man, D., et al., Intelligent intrusion detection based on federated learning for edge-assisted Internet of Things. Security and Communication Networks, 2021. 2021.

105. Rajendran, S., et al., Cloud-based federated learning implementation across medical centers. JCO clinical cancer informatics, 2021. 5: p. 1-11.

106. Said, O.; Tolba, A. Accurate performance prediction of IoT communication systems for smart cities: An efficient deep learning-based solution. Sustain. Cities Soc. 2021, 69, 102830.

107. Rieke, N., et al., The future of digital health with federated learning. NPJ digital medicine, 2020. 3(1): p.1-7.

108. Kim, J.; Kim, J.; Thu, H.L.T.; Kim, H. Long short-term memory recurrent neural network classifier for intrusion detection. In Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 15–17 February 2016; pp. 1–5.

109. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Appl. Sci. 2019, 9, 4396.

110. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 2015, 18, 1153–1176.

111. Pajouh, H.H.; Javidan, R.; Khayami, R.; Ali, D.; Choo, K.K.R. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg. Top. Comput. 2016, 7, 314–323.

112. Ghosh, P.; Mitra, R. Proposed GA-BFSS and logistic regression based intrusion detection system. In Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, India, 7–8 February 2015; pp. 1–6.

113. Prokofiev, A.O.; Smirnova, Y.S.; Surov, V.A. A method to detect Internet of Things botnets In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 29 January–1February 2018; pp. 105–108.

114. Azad, C.; Mehta, A.K.; Jha, V.K. Evolutionary Decision Tree-Based Intrusion Detection System. In Proceedings of the Third International Conference on Microelectronics, Computing and Communication Systems; Springer: Berlin/Heidelberg, Germany, 2019; pp. 271–282.

115. Kumar, V.; Das, A.K.; Sinha, D. UIDS: A unified intrusion detection system for IoT environment. Evol. Intell. 2021, 14, 47–59.

116. Amarasinghe, K.; Manic, M. Improving user trust on deep neural networks based intrusion detection systems. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 3262–3268.

117. Blanco, R.; Cilla, J.J.; Malagón, P.; Penas, I.; Moya, J.M. Tuning cnn input layout for ids with genetic algorithms. In Proceedings of the International Conference on Hybrid Artificial Intelligence Systems, Oviedo, Spain, 20–22 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 197–209.

118. Diro, A.; Chilamkurti, N. Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Commun. Mag. 2018, 56, 124–130.

119. HaddadPajouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.K.R. A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. Future Gener. Comput. Syst. 2018, 85, 88–96.

120. Huong, T.T., et al., Lockedge: Low-complexity cyberattack detection in iot edge computing. IEEE Access, 2021. 9: p. 29696-29710.

121. Preuveneers, D., et al., Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences, 2018. 8(12): p. 2663.

122. Ashraf, E.; Areed, N.F.F.; Salem, H.; Abdelhay, E.H.; Farouk, A. FIDChain: Federated Intrusion Detection System for BlockchainEnabled IoT Healthcare Applications. Healthcare 2022, 10, 1110. https://doi.org/10.3390/healthcare10061110